FILED ENTERED
LOGGED RECEIVED

MAY 02 2017

AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNTS: **kavasko.loren@gmail.com, kavasko.alex@gmail.com, kcautogallery@gmail.com, and EIExtraIncome@gmail.com** **THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.**	)	**Case No.** 17-883-CBD

AFFIDAVIT

I, Jeremy J. Brown, being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (the **Target Accounts**) that is stored at premises controlled by **Google, Inc. (Google)**, an email provider headquartered **Google, 1600 Amphitheatre Parkway, Mountain View, CA 94043**. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Google** to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a **Special Agent (SA)** with the **United States Secret Service (USSS)**, and have been since September 23, 2002. I am presently assigned to the Criminal Investigative Division, Asset Forfeiture Branch, Washington, D.C. I have received training and instruction in

JJB
CBD

federal criminal laws and fraud involving federally insured financial institutions at the Federal Law Enforcement Training Center in Glynco, Georgia, and the James J. Rowley Training Center in Beltsville, Maryland. I have experience in investigating violations of federal law relating to fraud involving federally insured financial institutions and private financial institutions. I have experience in executing search warrants and seizing evidence of federal criminal violations relating to fraud involving federally insured and private financial institutions and fraud involving the use of interstate wire communications. I have extensive experience in investigating crimes involving bank fraud and loan fraud as it relates to automobile purchases. I am authorized under 18 U.S.C. § 3056(b) to conduct criminal investigations concerning potential violations of 18 U.S.C. § 1014 or potential violations of the laws of the United States concerning fraud or other criminal activity against any federally insured financial institution. I am further authorized by 18 U.S.C. § 3056(c) to execute warrants issued under the laws of the United States and make arrests, either with or without a warrant, based upon probable cause, for any felony cognizable under the laws of the United States.

3. I have prepared this affidavit through conversations with other Special Agents to include a Special Agent in the USSS Criminal Investigative Division who has received specialized training from the USSS in the areas of electronic evidence handling, computer crimes, and cyber forensics and has received the designation Electronic Crimes Special Agent Program and has experience in the investigation of electronic/computer crimes and forensic handling of electronic evidence to include e-mail, the Internet, and stored electronic communications.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information

contained in this affidavit is based upon my personal knowledge, review of documents and other evidence, and conversations with other law enforcement officers and other individuals. All conversations and statements described in this Affidavit are related in substance and in part unless otherwise indicated. This affidavit contains information necessary to establish probable cause to believe that the **Target Accounts** contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1014 (Loan Application Fraud), 1344 (Bank Fraud), and 1349 (Bank Fraud Conspiracy).

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated," pursuant to 18 U.S.C. § 2711(3)(A)(i).

TRAINING AND EXPERIENCE

6. Based upon my training and experience, your affiant knows that:

a. It is common for individuals involved in financial crimes to maintain financial documents and records relating to their personal and business affairs. These documents will show the acquisition, conversion, movement, secretion, transfer, and distribution of currency, real property, and personal property. It is also common for such persons to maintain financial instruments that are the proceeds of, or facilitating property of, the illegal activity. These documents, records, and financial instruments are often retained for long periods of time in secure and accessible locations, including in their email accounts.

b. Based on the facts described below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1014 (Loan Application

Fraud), 1344 (Bank Fraud), and 1349 (Bank Fraud Conspiracy) will be found in the **Target Accounts**.

c. The records and documents created and retained by individuals involved in financial crime also often include correspondence with co-conspirators; U. S. Postal Service and/or next day carrier service documents and receipts; investor records; contracts; Rolodex files; photographs; appointment books; notes; airline and other travel tickets and receipts; bank account's records; and financial instruments. Individuals involved in financial crimes create such documents, records, and information by various means, including, but not limited to, computers, printers, telex machines, facsimile machines, and telephones, telephone answering machines, cellular phones, electronic tablets, external drives and cameras. These individuals also maintain such documents, records, and information in various forms, including but not limited to, electrical, magnetic, photographic, and tangible. It is common for individuals in the automobile sales and automobile financing professions to communicate with their clients, banks, recorders of deeds, title companies, lenders, and other real estate professionals through the use of electronic mail, telephone and first class mail or courier.It is common for individuals in the automobile sales and automobile financing profession to send and receive documents on behalf of their clients and/or automobile purchasers.

d. It is common for individuals involved in automobile loan fraud schemes to communicate with fellow co-conspirators and/or unsuspecting cooperators (including "straw purchasers") through electronic mail, telephone and first class mail or courier.

FACTS SUPPORTING PROBABLE CAUSE

7. In March 2015, USSS began a criminal investigation of KAVASKO CORPORATION, an automobile broker previously located at 8130 Boone Boulevard, Suite 240,

JB
CM

Vienna, Virginia 22182. The investigation began as a result of multiple complaints by financial institutions, as well as by purchasers of automobiles, to the Fairfax County (Virginia) Police Department (Fairfax County PD) and the Montgomery County (Maryland) Police Department (Montgomery County PD). Pursuant to their investigation, detectives with Fairfax County PD and Montgomery County PD uncovered an automobile straw purchasing scheme organized by Kerem Celem. Celem has owned and operated various companies known as: Kavasko Corporation; KC Financial Services Corporation; KC Auto Gallery; KC Marketing Services, LLC; and Adige, Inc., all of which operated in the Fairfax County area. These companies (hereinafter referred to collectively as KAVASKO) served as brokers for automobile purchases of high-end vehicles, primarily Land Rovers and BMWs, which were purchased by straw purchasers who obtained loans from various financial institutions to purchase the vehicles.

8. On December 21, 2016, a Grand Jury in the District of Maryland returned an indictment charging: (1) Celem, Thomas Hardin Firth, Michael John Stoll, Brian Albert Armstrong, and Dimitrios Balourdos with bank fraud conspiracy, in violation of 18 U.S.C. § 1349; (2) Firth, Stoll, Armstrong, and Balourdos with bank fraud, in violation of 18 U.S.C. § 1344; and (3) Firth and Stoll with false statement on a loan application, in violation of 18 U.S.C. § 1014.

9. As alleged in the Indictment, KAVASKO employees recruited, at job fairs and other locations, straw purchasers or purchasing agents to purchase luxury vehicles at various car dealerships on behalf of KAVASKO. Indictment (ECF 1) ¶¶ 16 & 18. The Indictment alleges that the straw buyers entered into "Non Exclusive Purchasing Agency Agreements" with KAVASKO, which agreements provided that the purchasing agent (the straw buyer) would purchase a luxury vehicle using KAVASKO's "own funds" and the straw buyers' "credit worthiness" to do so. As alleged in the Indictment, the straw buyers agreed, at the direction of KAVASKO and immediately

on full payment of the automobile loan, to transfer title of the vehicle to KAVASKO. *Id.* at ¶¶ 19 & 20. Despite this agreement, KAVASKO eventually stopped making payments on the vehicle loans obtained by the straw buyers, causing the loans to go into default. *Id.* at ¶ 30. The Purchasing Agency Agreement, which was executed without the knowledge of the victim financial institution, further states that absolute title to all automobiles purchased by the straw purchaser would immediately vest in KAVASKO.

10. The Indictment further alleges that the straw buyers obtained loans in their own names to finance the purchase of the vehicles on behalf of KAVASKO. The Indictment alleges that the straw buyers were instructed and caused to make false representations on the credit applications submitted to the financial institutions that funded the loan; these false and fraudulent representations included that the straw buyer was the true purchaser of the vehicle. *Id.* at ¶ 25. These fals and fraudulent representations also related to the straw buyers' salary and employment. *Id.* at ¶¶ 31.a. & 31.r. In some cases, straw buyers listed as their employer a company owned or controlled by Celem or another co-conspirator, such as Adige, Inc., Florida Regional Gateway, and Community Realty and Investments.

11. Moreover, the Indictment alleges that the straw buyers signed Retail Installment Sale Contracts, which were assigned to the Financial Institutions by the car dealerships and which provided, "You agree not to remove the vehicle from the U.S. or Canada, or to sell, rent, lease, or transfer any interest in the vehicle or this contract without our written permission." Despite this provision, the straw buyers quickly resold the cars to KAVASKO after the purchase from the dealerships, without obtaining the written permission of the financial institutions. KAVASKO thereafter sold the vehicles to various companies, knowing that the vehicles would be exported outside the United States without first obtaining the written permission from the financial

institutions. *Id.* at ¶¶ 26, 27 & 28.

12. The Indictment further alleges that, when a vehicle was to be purchased by Manhattan Imported Cars (identified as Dealership A in the Indictment), Balourdos served as the sales representative on the transaction and Armstrong ensured that a loan was approved for the purchase and that the sale was completed. *Id.* at ¶ 23.

13. On December 2, 2015, I interviewed Alexandrea Dunford, a former employee of KAVASKO's who provided the following information: Dunford's employment with Kavasko began primarily as a receptionist. She later was tasked with calling various dealerships to determine what types of automobiles they had in their inventory. In the Spring of 2014, Dunford moved to a new office where she began recruiting straw purchasers at job fairs and shows. They used flyers that described purchasing cars for re-sale and omitted anything about loans. Dunford further indicated that she communicated with straw purchasers and other Kavasko employees using **Target Account kavasko.alex@gmail.com**.

14. On December 8, 2015, I interviewed Loren Grimes, a former employee of KAVASKO's who provided the following information: After a couple of weeks working for KAVASKO, Grimes began recruiting straw purchasers at job fairs. Grimes further indicated that she communicated with straw purchasers and other Kavasko employees using **Target Account kavasko.loren@gmail.com**. Grimes also indicated that Celem used **Target Account kcautogallery@gmail.com**.

15. KAVASKO employee and indicted coconspirator Michael John Stoll interacted with several straw purchasers through email, including Person A and the straw buyer identified as Co-conspirator 1 in the Indictment. I interviewed Person A, who provided e-mails exchanged between himself and Stoll, who was using **Target Account EIExtraIncome@gmail.com**. The

emails concern the purchase of automobiles for KAVASKO. In one of these e-mails, Person A told Stoll that Person A was unaware that the automobile purchased would need to be financed in her name until the last minute, when Stoll explained the need to finance the automobile but promised that KAVASKO would take care of the loan payments. Co-conspirator 1 exchanged e-mails with Stoll at **Target Account EIExtraIncome@gmail.com** in December 2013 and December 2014 concerning the purchase of cars for KAVASKO. Co-conspirator 1 also provided me with a handwritten note bearing the signature "Alexandrea Dunford" concerning a check mailed for a loan payment, which was later returned for insufficient funds (NSF). Included on this handwritten note are the notations: "**kcautogallery@gmail.com**" (one of the **Target Accounts**) and "Thomas, (571) 480-0921," believed to refer to Firth.

16. On September 2, 2016, United States Magistrate Judge William Connelly, District of Maryland, issued a search warrant for the **Target Accounts**. *See* Attachment C, incorporated by reference. At my request, a USSS SA served this search warrant on **Google** via their Law Enforcement Request System (LERS). On September 22, 2016, **Google** notified the USSS SA via e-mail that **Google** had produced documents responsive to the search warrant; however, I did not receive notification of this production. From September 2016 through February 2017, I monitored the **Google** LERS for production of documents pursuant to the search warrant, but I did not receive any such notification from **Google** as to this production. On February 15, 2017, the USSS SA informed me that **Google** had notified him that **Google** had produced documents responsive to the search warrant on September 20, 2016, and that the documents were no longer available. **Google** further informed the USSS SSA that **Google** would require new legal process to produce the documents they previously had produced on September 20, 2016.

17. Preservation requests for the **Target Accounts** were sent to **Google** on December 7, 2015, and March 14, 2016. In general, an email that is sent to a **Google** subscriber is stored in the subscriber's "mail box" on **Google** servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on **Google** servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on **Google's** servers for a certain period of time.

18. Based on the facts articulated herein, I believe there is sufficient probable cause to conclude that stored within the **Target Accounts,** more specifically described in Attachment A hereto, there exists the information listed in Attachment B, Section II, hereto, such information constituting evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1014 (Loan Application Fraud), 1344 (Bank Fraud), and 1349 (Bank Fraud Conspiracy).

BACKGROUND CONCERNING EMAIL

19. In my training and experience, I have learned that **Google** provides a variety of on-line services, including electronic mail ("email") access, to the public. **Google** allows subscribers to obtain email accounts at the domain name gmail.com, like the **Target l Accounts**. Subscribers obtain an account by registering with **Google**. During the registration process, **Google** asks subscribers to provide basic personal information. Therefore, the computers of **Google** are likely to contain stored electronic communications (including retrieved and un-retrieved email for **Google** subscribers) and information concerning subscribers and their use of **Google** services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. A **Google** subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by **Google**. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address

information can help to identify which computers or other devices were used to access the email account.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and

geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on **Google**, which will then compile the requested records at a time of day convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Jeremy J. Brown
Special Agent
United States Secret Service

Subscribed and sworn to before me on the 21st of March, 2017

Honorable Charles B. Day
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **kavasko.loren@gmail.com** and **kavasko.alex@gmail.com** and **EIExtraIncome@gmail.com** and **kcautogallery@gmail.com** that is stored at premises controlled by **Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1014 (Loan Application Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Wire and Bank Fraud Conspiracy), and 2314 (Interstate and foreign transportation of stolen goods), those violations involving **KEREM CELEM; MICHAEL STOLL; DIMITRIOS BALOURDOS; THOMAS FIRTH; LOREN GRIMES; ALEXANDREA DUNFORD; AND KAVASKO CORPORATION, KC AUTO GALLERY, KC MARKETING SERVICES, LLC, and ADIGE, INC. (HEREINAFTER REFERRED TO COLLECTIVELY AS KAVASKO CORPORATION)** and occurring after **November 1, 2012,** including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Records and information relating to a conspiracy to engage in bank fraud, wire fraud, loan application fraud, and transportation of stolen goods.

2. Records and information relating to:

   a. Manhattan Imported Cars, Inc.; and its employees and former employees, including Brian Armstrong, Dimitrios Balourdos, ~~and Augie Borges~~. CBS

   b. Purchasers and prospective purchasers of vehicles for or on behalf of KAVASKO CORPORATION.

   c. Non-Exclusive Purchasing Agency Agreements between KAVASKO CORPORATION and purchasers and prospective purchasers of vehicles for or on behalf of KAVASKO CORPORATION.

JJB
CBS

d. Vehicles (and their corresponding VINs) purchased by a straw purchaser or pursuant to a Non-Exclusive Purchasing Agency Agreement with KAVASKO CORPORATION.

e. Personally identifiable information (PII) for any and all straw purchasers, including but not limited to their: Social Security Number (SSN), date of birth (DOB), address, bank account number(s), etc.

f. Income and employment information for any and all prospective and actual straw purchasers.

g. Adige, Inc.; Florida Gateway Regional; Community Realty and Investments.

h. Any and all companies owned or controlled by Kerem Celem.

i. Automobile credit applications, customer profile information documents submitted to prospective lenders and/or automobile dealerships, proof of employment information, proof of income information (such as pay stubs, income tax returns, W-2s, etc.), credit reports, automobile loan installment contracts, automobile loan funding disbursements (bank wires, checks, ACH deposit records, etc.), and any and all documents/records concerning automobile purchases, automobile financing and/or automobile loans.Correspondence between KAVASKO CORPORATION and prospective or actual "purchasing agents," that is, automobile purchasers and borrowers acting on behalf of and under the direction of KAVASKO CORPORATION (i.e., straw purchasers), including but not limited to the following: "Non-Exclusive Purchasing Agent Agreements," e-mail and text/iMessage/SMS messages concerning the purchase of automobiles by straw purchasers, and letters and correspondence to/from straw purchasers and KAVASKO CORPORATION concerning re-payment of loans on automobiles purchased by straw purchasers.

j. Correspondence between KAVASKO CORPORATION ration and Manhattan Imported Cars, Inc.; Sales Manager Brian Armstrong; ~~Finance Manager Nicholas Cusato~~; salesman Dimitrios Balourdos; and salesman ~~Augie Borges~~, including but not limited to: e-mail and text/iMessage/SMS messages, letters, and correspondence.

k.

Loan re-payments by KAVASKO CORPORATION on automobile loans on behalf of straw purchasers, including but not limited to following: checks, ACH transactions, wire transfers, and correspondence from financial institutions concerning said re-payments.

a. Bank accounts maintained or used by KAVASKO CORPORATION, including but not limited to records relating to deposits and wire transfers into those accounts and disbursements from those accounts.
b. Towing, shipping, and/or export of the vehicles overseas.
c. Agreements between KAVASKO CORPORATION and any automobile dealership or automobile dealership employee.
d. Payments by KAVASKO CORPORATION to any automobile dealership or automobile dealership employee in connection with the purchase or sale of a vehicle by a straw purchaser.

3. Payments by KAVASKO CORPORATION to any automobile dealership or automobile employee in connection with the export of a vehicle overseas.Any and all correspondence, e-mail, text/iMessage/SMS messages between and among KAVASKO CORPORATION, its employees, agents, and associates (including Kerem Celem, Thomas Firth, Michael Stoll, ~~Ahmet Emre Kuzudisli, David Williams~~, Loren Grimes, ~~Jessica Jimenez~~, Alexandra Dunford, ~~Cagdas "Josh" Cimen, and Anthony Raymond~~) related to items 2.a.-2.q.

4. Any and all photographs of currency, cashier's checks, other financial documents, vehicles, and/or KAVASKO CORPORATION employees, agents, and associates (including Kerem Celem, Thomas Firth, Michael Stoll, Ahmet Emre Kuzudisli, David Williams, Loren Grimes, Jessica Jimenez, Alexandra Dunford, Cagdas "Josh" Cimen, and Anthony Raymond).

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form, stored on the account listed on Attachment A hereto.

5. The following types of information pertaining to user(s) of the account listed on the attachment A hereto:

a. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

b. Evidence indicating the email account owner's state of mind as it relates to the crime(s) under investigation;

c. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

JB
CBD